

EXPLICIT REQUEST FOR  
MORE CAREFUL ATTENTION TO ACTUAL CLAIM LANGUAGE

The Office Action dated July 16, 2007 fails to address the actual language of the claims. Specifically, the Office Action enters rejections based on language found in earlier versions of the claims, but not based on language in the then-current versions of the claims. Thus, the Office Action enters rejections based on language not apparently found in the claims, and also fails to address language that is actually there.

For example, in connection with its rejection of Claim 26, found on page 3, the Office Action explained why it believes that the Rosenow patent includes a reception unit. However, the language used in rejecting Claim 26 is not the same as the actual language of Claim 26, as shown below in a side-by-side comparison:

Claim Language Rejected in the Office  
Action Dated July 16, 2007

a reception unit constructed to receive, from a computer, a job and access management information for identifying a feature and/or a service of the device available to a user (i.e.: a private means or identifying a feature and/or a service of the device not available to the user), wherein the access management information is transmitted from a server to the computer [Rosenow, providing a private and dedicated means of transferring access management data from CACS to all access controllers (or peripheral devices) on an as-needed basis, col. 8 lines 10-15]; and

Actual Claim Language as Amended in  
the Amendment Dated June 26, 2007

a reception unit constructed to receive, from a computer, a job and access management information ~~for identifying~~ which identifies a feature and/or a service of the device available to a user or ~~identifying~~ a feature and/or a service of the device not available to the user, wherein the access management information is transmitted from a server to the computer before the access management information is transmitted from the computer to the device; and

Note that the above comparison reproduces claim language in the same format as that shown in the Amendment dated June 26, 2007, including markups that indicate language deleted from the claim and language added to the claim. Note further that the rejection omits any discussion of Claim 26's temporal feature, namely, that the access management information is transmitted from a sever to a computer before the access management information is transmitted from the computer to the device.

Likewise, in its rejection of Claim 31, page 5 of the Office Action also fails to address actual language found in the claims:

Claim Language Rejected in the Office  
Action Dated July 16, 2007

a reception unit constructed to receive, from a computer, a job and access management information for identifying a feature and/or a service of the device available to a user, wherein the access management information is transmitted from a server to the computer [Rosenow, providing a private and dedicated means of transferring access management at a from CACS to all access controllers on an as-needed basis, col 8 lines 10-15]; and

Actual Claim Language as Amended in  
the Amendment Dated June 26, 2007

a reception unit constructed to receive, from a computer, a job and access management information ~~for identifying~~ which identifies a feature and/or a service of the device available to a user, wherein the access management information is transmitted from a server to the computer before the access management information is transmitted from the computer to the device; and

Thus, the Office Action fails to address actual language of the current claims, but rather incorrectly addresses language found in prior versions of the claims.

With respect, it is pointed out that this failure to address actual claim language has happened before in this case. Specifically, the Office Action dated October 25, 2005 failed to address then-current claim language, but rather incorrectly addressed

earlier versions of the claims. The Office Action was therefore withdrawn, pursuant to a request filed on November 17, 2005.

Likewise, the Office Action dated January 10, 2006 failed to address then-current language of the claims, but rather incorrectly addressed prior versions of the claims. The Office Action was therefore withdrawn, pursuant to an agreement reached at an interview conducted on February 23, 2006.

Other Office Actions have also failed to address then-current versions of the claims, even though this was not explicitly brought to the attention of the Examiner, or made part of the written record.

In view of the PTO's continued failure to address actual language of claims, it was felt that this extraordinary filing was warranted. Accordingly, it is respectfully requested for the PTO to give more careful attention to actual language of the claims, including the language of the current amendment. It is also respectfully requested for the PTO to explain any continued rejections of the claims with respect to the actual language thereof.

## REMARKS

This application has been carefully reviewed in light of the Office Action dated July 16, 2007. Claims 17 to 43 are in the application, of which the following claims are independent: Claims 17, 25, 26, 31, 32, 34 and 35. Reconsideration and further examination are respectfully requested.

The Office Action entered a rejection of Claims 17 to 36 under 35 U.S.C. § 102(b) over U.S. Patent 5,483,596 (Rosenow). The rejections are respectfully traversed, as explained in more detail below.

### Claim 17

The invention defined by Claim 17 concerns a method for controlling access to a peripheral device by a user, wherein the peripheral device is accessible by the user based on access management information, and wherein the peripheral device is constructed to provide the user with a plurality of features and/or services including at least one of a printer service, a scanner service, a facsimile service, and a copy service. According to the method defined by Claim 17, access management information is received at a computer from the server. The access management information specifies a feature and/or service of the peripheral device available to the user from among the plurality of features and/or services of the peripheral device, or specifies a feature and/or service of the peripheral device not available to the user from among the plurality of features and/or services of the peripheral device. The access management information is received at the peripheral device

from the computer. In addition, a job is received at the peripheral device from the computer. At the peripheral device, there is a determination as to whether the user can use the feature and/or the service of the peripheral device necessary to perform the receive job, based on the received access management information. In a case where it is determined that the user can use the feature and/or the service necessary to perform the receive job, the peripheral device performs the receive job.

Accordingly, in one aspect, there is specification of features and/or services available to the user from among a plurality of features and/or services of a peripheral device which include at least one of a printer service, a scanner service, a facsimile service and a copy service. In addition, this specification of features and/or services is based on access management information.

For example, as described in the specification in terms of one representative embodiment of the invention, the access management information may indicate a feature available to a user from among plurality of features of a printer service, for example, color or black-and-white printing. Also, when there is more than one service for the peripheral device, the access management information indicates a service available to the user, such as a copy service or a printer service. Further, the computer sends the access management information with a job to the peripheral device, and the peripheral device determines whether or not to perform the job based on the received access management information.

On the other hand, in the cited patent to Rosenow, encrypted data is sent to a computer of another user, and is decrypted at the computer. Rosenow therefore fails to disclose that there is a specification of features and/or services of a peripheral device, and

that such a specification is based on access management information. Further, Rosenow is not seen to disclose that it is the computer who sends the access management information and the job, nor is it seen to disclose the determination of whether or not the features and/or services can be executed to perform the received job, based on received access management information.

The Office Action nevertheless maintains its prior position that Rosenow's "access management data" corresponds to the claimed "access management information which specifies a feature and/or service that is available to a user". Applicants continue to traverse this interpretation of Rosenow, for at least two reasons. First, Rosenow's "access management data" could not possibly correspond to the claimed "access management information" since it is not transmitted from a server to a computer and thence from a computer to a peripheral device. Rather, Rosenow's access management data is consumed by Rosenow's access controller 16, and is not thereafter transmitted anywhere. This can be understood by reference to Rosenow's column 8, lines 22 to 48. Specifically, as explained in this cited portion of column 8, although Rosenow's access management data is transmitted from CACS server 58 to an access controller when it is newly-manufactured, it is not thereafter transmitted from the access controller to the device. Instead, it is the access controller itself that uses the access management data, so as to encrypt data to be sent to the device. Thus, Rosenow's access controller does not send the access management data to the device, but rather consumes the access management data by itself.

Second, Rosenow's access management data does not correspond to the claimed access management information for the reason that since it is not sent to the

peripheral device, it is also not received by the peripheral device and thus cannot be used by the peripheral device to determine whether a user can use a feature and/or service of the device necessary to perform a received job.

Moreover, in the context of the amendments made herein, it should be understood that the features and/or services include at least one of a printer service, a scanner service, a facsimile service and a copy service. Thus, since the Rosenow disclosure concerns only encryption, and not one of the enumerated features and/or services, it stands to reason that Rosenow's access management data could not possibly correspond to the claimed access management information.

Page 2 of the Office Action also cites to the functionality of Rosenow's resource access control services system ("RACS") server 46. As understood from the explanation at page 2, the Office Action is taking the position that based on Figure 1 of Rosenow, RACS server 46 controls and provides resources or services to network devices or users. Applicants respectfully disagree with this explanation. Specifically, Rosenow's column 7 provides a clear description of the functionality of RACS server 46. According to the description at column 7, RACS server 46 provides resources and services to access controllers, and not to network devices or users.

In light of all of these deficiencies of Rosenow, it is respectfully submitted that Rosenow could not possibly be anticipatory, under § 102(b), of the subject matter of Claim 17. Withdrawal of the rejection is respectfully requested.

### Claim 25

The invention defined by Claim 25 concerns a method for controlling access to a peripheral device by a user, wherein the peripheral device is accessible by the user based on access management information, and wherein the peripheral device is constructed to provide the user with a plurality of features and/or services including at least one of a printer service, a scanner service, a facsimile service, and a copy service. According to the method defined by Claim 25, access management information is received at a computer from a server, wherein the access management information specifies a feature and/or service of the peripheral device available to the user from amongst the plurality of features and/or services of the peripheral device. The access management information is thereafter received at the peripheral device from the computer. In addition, a job is received at the peripheral device from the computer. The peripheral device makes a determination as to whether the user can use the feature and/or the service of the peripheral device necessary to perform the received job, based on the received access management information. In a case where it is determined that the user can use the feature and/or service necessary to perform the receive job, the peripheral device performs the job.

Thus, according to one feature of Claim 25, the access management information is received at a computer from a server, and the access management information is then received at the peripheral device from the computer.

According to a further aspect of the invention, it is the peripheral device that makes a determination, based on the access management information received by it, as to



whether the user can use the feature and/or the service of the peripheral device necessary to perform a receive job.

According to a further feature of Claim 25, the access management information specifies a feature and/or a service from amongst a plurality of features and/or services that include at least one of a printer service, a scanner service, a facsimile service, and a copy service.

Rosenow is not seen to disclose or to suggest the features of Claim 25, and is specifically not seen to disclose or to suggest the above-noted features. Specifically, Rosenow's access management data is not seen to specify a feature and/or a service of a peripheral device which includes at least one of a printer service, a scanner service, a facsimile service, and a copy service. Additionally, Rosenow's access management data is not received at a computer from a server and thereafter also received at the peripheral device from the computer. Rather, Rosenow's access management data is consumed by his access controller, which does not thereafter forward it anywhere. Furthermore, because the peripheral device does not receive Rosenow's access management data, it is not possible for the peripheral device to make a determination as to whether the user can use a feature and/or service of the peripheral device, based on received access management information.

It is therefore respectfully submitted that Claim 25 is fully in condition for allowance.

## Claim 26

Claim 26 defines a peripheral device which is accessible by a user based on access management information. The peripheral device is constructed to provide the user with a plurality of features and/or services including at least one of a printer service, a scanner service, a facsimile service, and a copy service. As defined by Claim 26, the peripheral device comprises a reception unit constructed to receive, from a computer, access management information, wherein the access management information specifies a feature and/or service of the peripheral device available to the user from among the plurality of features and/or services of the peripheral device, or specifies a feature and/or a service of the peripheral device not available to the user from among the plurality of features and/or services of the peripheral device. This access management information is transmitted from a server to the computer before the access management information is also transmitted from the computer to the device.

The reception unit is also constructed to receive a job from the computer. A controller is constructed to determine, based on the received access management information, whether the user can use the feature and/or the service of the peripheral device necessary to perform the received job, and is also constructed to perform the received job in a case that it is determined that the user can use the feature and/or the service necessary to perform the received job.

Rosenow's access management data is not seen to correspond to the claimed access management information. First, Rosenow's access management data does not specify a feature and/or a service of a peripheral device which includes a plurality of

features including at least one of a printer service, a scanner service, a facsimile service, and a copy service. Second, Rosenow's access management data is not ever received at a peripheral device, but rather stops permanently at his access controllers. Thus, Rosenow's access management data is not transmitted from a server to a computer before it is thereafter transmitted from the computer to the peripheral device. Third, because Rosenow's access management data is not received at the peripheral device, the peripheral device cannot make a determination, based on received access management information, as to whether the user can use the feature and/or the service of the peripheral device necessary to perform a received job.

Withdrawal of the rejection of Claim 26 is respectfully requested.

#### Claim 31

Claim 31 defines peripheral device which is accessible by a user based on access management information, wherein the peripheral device is constructed to provide the user with a plurality of features and/or services including at least one of a printer service, a scanner service, a facsimile service, and a copy service. The peripheral device defined by Claim 31 comprises a reception unit constructed to receive access management information, which is received from a computer. The access management information specifies a feature and/or a service of the peripheral device available to the user from among the plurality of features and/or services of the peripheral device. The access management information is transmitted from a server to the computer before the access management information is transmitted from the computer to the peripheral device. A job

is also received from the computer. A controller determines, based on the received access management information, whether the user can use the feature and/or the service of the peripheral device necessary to perform the received job, and performs the received job in a case where it is determined that the user can use the feature and/or the service necessary to perform the received job.

Rosenow is not seen to disclose or to suggest the above features of independent Claim 31. Specifically, Rosenow's access management data does not correspond to the claimed access management information, since Rosenow's access management data does not pertain to, or otherwise "specify", a feature and/or service of the peripheral device which includes a plurality of features and/or services including at least one of a printer service, a scanner service, a facsimile service, and a copy service. In addition, Rosenow's access management data is not received by a peripheral device, for the reason that it is consumed by Rosenow's access controller. Accordingly, Rosenow's access management data is not transmitted from a server to computer before the access management data is thereafter transmitted from the computer to the peripheral device. Furthermore, because Rosenow's peripheral device never receives its access management data, it is not possible for Rosenow's peripheral device to make a determination, based on such access management data, whether a user can use the feature and/or the service of the peripheral device necessary to perform the received job.

Allowance of Claim 31 is respectfully requested.

### Claim 32

Claim 32 defines a server for use in controlling access to a peripheral device by a user. The peripheral device is accessible by the user based on access management information, wherein the peripheral device is constructed to provide the user with a plurality of features and/or services including at least one of a printer service, a scanner service, a facsimile service, and a copy service. The server of Claim 32 comprises a reception unit constructed to receive authentication information corresponding to a user from a computer, and an authentication unit is constructed to authenticate the user using the received authentication information. A transmission unit transmits access management information to the computer, wherein the access management information specifies a feature and/or service of the peripheral device accessible to the authenticated user from among the plurality of features and/or services of the peripheral device, or specifies a feature and/or service of the peripheral device not available to the authenticated user from among the plurality of features and/or services of the peripheral device. The computer transmits the access management information and a job to the peripheral device. The peripheral device makes a determination, based on the transmitted access management information, whether the user can use the feature and/or the service of the peripheral device necessary to perform the job. The peripheral device thereafter performs the job in the case that it is determined that the user can use the feature and/or the service necessary to perform the job.

Rosenow is not seen to disclose or to suggest the foregoing features of Claim 32. Specifically, Rosenow is not seen to disclose or to suggest a server that

authenticates a user by using authentication information corresponding to a user, and thereafter transmits to the computer access management information which specifies a feature and/or a service of a peripheral device that is available to an authenticated user. In addition, Rosenow's access management data is not seen to correspond to the claimed access management information, for the reason that Rosenow's access management data does not specify a feature and/or service of a peripheral device which includes a plurality of features and/or services including one of a printer service, a scanner service, a facsimile service, and a copy service. Furthermore, Rosenow's access management data is not transmitted from a server to a computer and thence by a computer to a peripheral device. Accordingly, since Rosenow's access management data is not received by a peripheral device, it is also not possible for any of Rosenow's peripheral devices to make a determination as to whether a user can use the feature and/or the service of the peripheral device necessary to perform the received job, based on access management information.

It is therefore respectfully submitted that Claim 32 is fully in condition for allowance.

#### Claim 34

Independent Claim 34 concerns a server for use in controlling access to a peripheral device by a user, wherein the peripheral device is accessible by the user based on access management information, and wherein the peripheral device is constructed to provide the user with a plurality of features and/or services including at least one of a printer service, a scanner service, a facsimile service, and a copy service. According to the

server defined by Claim 34, a reception unit is constructed to receive authentication information corresponding to a user from a computer, and an authentication unit is constructed to authenticate the user using the transmitted authentication information. A transmission unit transmits access management information to the computer, wherein the access management information specifies a feature and/or a service of the peripheral device available to the authenticated user from among the plurality of features and/or services of the peripheral device. The computer transmits the access management information and a job to the peripheral device. The peripheral device determines, based on the transmitted access management information, whether the user can use the feature and/or the service of the peripheral device necessary to perform the job. The peripheral device thereafter performs the job in the case that it is determined that the user can use the feature and/or the service necessary to perform the job.

Rosenow is not seen to disclose or to suggest the foregoing features of Claim 34. Specifically, Rosenow is not seen to disclose or to suggest a server that authenticates a user by using authentication information corresponding to a user, and thereafter transmits to the computer access management information which specifies a feature and/or a service of a peripheral device that is available to an authenticated user. In addition, Rosenow's access management data is not seen to correspond to the claimed access management information, for the reason that Rosenow's access management data does not specify a feature and/or service of a peripheral device which includes a plurality of features and/or services including one of a printer service, a scanner service, a facsimile service, and a copy service. Furthermore, Rosenow's access management data is not

transmitted from a server to a computer and thence by a computer to a peripheral device. Rather, Rosenow's access management data stops at his access controllers, which do not forward the access management data on to peripherals. Accordingly, since Rosenow's access management data is not received by a peripheral device, it is also not possible for any of Rosenow's peripheral devices to make a determination as to whether a user can use the feature and/or the service of the peripheral device necessary to perform the received job, based on access management information.

It is therefore respectfully submitted that Claim 34 is fully in condition for allowance.

#### Claim 35

Claim 35 pertains to a computer for transmitting a job to a peripheral device. The peripheral device is accessible by a user based on access management information, and is constructed to provide the user with a plurality of features and/or services including at least one of a printer service, a scanner service, a facsimile service, and a copy service. This computer as defined by Claim 35 includes a reception unit constructed to receive access management information from a server, wherein the access management information specifies a feature and/or a service of the peripheral device available to the user from among the plurality of features and/or services of the peripheral device, or specifies a feature and/or a service of the peripheral device not available to the user from among the plurality of features and/or services of the peripheral device. A transmission unit transmits the transmitted access management information to the



peripheral device, and also transmits a job to the peripheral device. The peripheral device determines whether the user can use the feature and/or the service of the peripheral device necessary to perform the job, based on the transmitted access management information. The peripheral device performs the job in a case that it is determined that the user can use the feature and/or the service necessary to perform the job.

Thus, in the context of the invention, which involves cooperative interaction between a computer, a server, and a peripheral device, wherein access management information is transmitted from the server to the computer, and wherein the access management information and a job is thereafter transmitted from the computer to the peripheral device, Claim 35 defines the nature of the computer.

Rosenow is not seen to disclose or to suggest the subject matter of Claim 35. Specifically, Rosenow's access management data is not seen to correspond to the claimed access management information, for the reason that access management data does not specify a feature and/or service of a peripheral device which is constructed to provide a plurality of features and/or services including at least one of a printer service, a scanner service, a facsimile service, and a copy service. Rosenow's access management data is also not seen to be transmitted to a peripheral device, unlike the invention which involves the transmission of access management information from a server to a computer, and thence from a computer to the peripheral device. Furthermore, since Rosenow's access management data is not received at a peripheral device, it is not possible for Rosenow's peripheral device to make a determination as to whether the user can use the feature and/or

the service of the peripheral device necessary to perform a received job, based on such access management data.

Allowance of Claim 35 is respectfully requested.

CONCLUSION

Applicants' undersigned attorney may be reached in our Costa Mesa, California Office by telephone at (714) 540-8700. All correspondence should be directed to our address given below.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Michael K. O'Neill", written over a horizontal line.

Attorney for Applicants  
Michael K. O'Neill  
Registration No.: 32,622

FITZPATRICK, CELLA, HARPER & SCINTO  
30 Rockefeller Plaza  
New York, New York 10112-3800  
Facsimile: (212) 218-2200

FCHS\_WS 1666218v1